



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



050.103 System's Security Plan

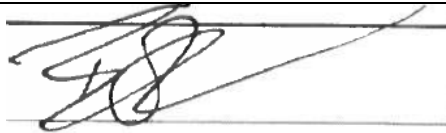

**Version 1.2
February 19, 2018**

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

Revision History

Date	Version	Description	Author
4/29/2016	1.1	Effective Date	CHFS IT Policies Team Charter
2/19/2018	1.2	Revision Date	CHFS OATS Policy Charter Team
2/19/2018	1.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	2/19/2018	Bernard "Deck" Decker	
CHFS Chief Information Security Officer (or designee)	2/19/2018	DENNIS B. LEEGER	

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

Table of Contents

050.103 SYSTEM'S SECURITY PLAN	5
1 POLICY OVERVIEW	5
1.1 PURPOSE	5
1.2 SCOPE	5
1.3 MANAGEMENT COMMITMENT	5
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.5 COMPLIANCE	5
2 ROLES AND RESPONSIVITIES	6
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	6
2.2 SECURITY/PRIVACY LEAD	6
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	6
2.4 CHFS STAFF AND CONTRACT EMPLOYEES	6
3 POLICY REQUIREMENTS	7
3.1 SYSTEM SECURITY PLAN	7
3.2 RULES OF BEHAVIOR	8
3.3 INFORMATION SECURITY ARCHITECTURE	8
4 POLICY MAINTENANCE RESPONSIBILITY	8
5 POLICY EXCEPTIONS	8
6 POLICY REVIEW CYCLE	8
7 POLICY REFERENCES	8

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

Policy Definitions

- **Agency:** for the purpose of this document, agency or agencies refers to any department under the Cabinet of CHFS.
- **Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects (people, systems, or devices). The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Rules of Behavior:** security control contained in NIST SP 800-53, should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for access to the system. It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

050.103 System's Security Plan

Category: 050.000 Security Awareness

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a security planning policy. This document establishes the System's Security Planning Policy which helps manage risks and provides guidelines for security best practices regarding security planning, preparation, and strategy.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restricted access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

2 Roles and Responsivities

2.1 Chief Information Security Officer (CISO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contract Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

3 Policy Requirements

3.1 System Security Plan

CHFS OATS must develop and maintain a System Security Plan (SSP) for the agency's information system. An approved and accurate System Security Report (SSR), from the IRS satisfies the requirement for a SSP, for those applications that use Federal Tax Information (FTI).

This plan must delineate responsibilities and expected behavior of all individuals who access the applications. The SSP/SSR shall be viewed as documentation and processes for the security protections of information systems, including those that contact FTI.

The agency must develop a system security plan that includes, but is not limited to, the following guidelines:

1. A plan that is consistent with the organization's enterprise architecture
2. A plan that explicitly defines the authorization boundary for the system
3. A plan that describes the operational context of the information system in terms of missions and business processes
4. A plan that provides the security categorization of the information system including supporting rationale
5. A plan that describes the operational environment for the information system and relationships with or connections to other information systems
6. A plan that provides an overview of the security requirements for the system
7. A plan that identifies any relevant overlays, if applicable
8. A plan that describes the security controls in place or planned for meeting those requirements including a rationale for tailoring decisions
9. A plan that is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

The SSP/SSR will be reviewed at least annually or more often if there are major changes in the system. The agency will share the plan updates and changes with all necessary agency management staff as needed or upon request. An example/template of how to create a Information System Security Plan can be found within Appendix A of the National Institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems: Appendix A.

Reasons for changes or updates to the plan may include, but are not limited to:

1. Changes to the information systems
2. Change to the environment of operations
3. Change or updates to security controls in place
4. Problems identified during plan implementations or security control assessments
5. Other major releases or changes to the system or application

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

Agencies may develop procedures to plan and coordinate security related activities regarding the information system with affected stakeholders before conducting such activities to reduce the impact on other organizational entities.

3.2 Rules of Behavior

CHFS OATS establishes, provides, describes, and makes readily available the responsibilities and expected behavior of individuals who require access to the information system.

Upon hire, gaining access to the agency system, and every year thereafter, individuals are required to sign an acknowledgement form- such as the CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS 219)- agreeing that they have read, understood, and agree to abide by the rules of behavior before accessing the system or application.

3.3 Information Security Architecture

The agency will develop the information security architecture for the information system. This architecture will describe the overall requirements of how the agency plans to protect the confidentiality, integrity, and availability of the information. This security architecture will be updated to reflect updates in the enterprise architecture. All changes and updates will be documented in the SSP/SSR, when applicable.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Employee Privacy and Security of Protected Health Confidentiality, and Sensitive Information Agreement (CHFS-219)
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy

050.103 System's Security Plan	Current Version: 1.2
050.000 Security Awareness	Review Date: 02/19/2018

- CHFS OATS Procedure: CHFS System's Security Plan Procedure
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information